UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

SCHNUCK MARKETS, INC.,	)	
Plaintiff,	)	
v.	)	Case No. 4:13CV2226 JAR
FIRST DATA MERCHANT DATA SERVICES CORP., and CITICORP PAYMENT SERVICES, INC.	)	
Defendants.	)	

PLAINTIFF SCHNUCK MARKETS, INC.'S RESPONSE TO DEFENDANTS' SUR-REPLY MEMORANDUM

The Sur-Reply of Defendants/Counterclaim-Plaintiffs First Data and Citicorp (collectively, the "Defendants") is a continuation of their misdirection and confusion tactics. Their new arguments, which could have been made in their prior briefs but were not, do not withstand even minimal scrutiny.

To be fair, Defendants make two correct statements in the Sur-Reply, one is that Visa changed the name of its issuer loss liability program from Account Data Compromise Recovery (ADCR) to Global Compromised Account Recovery (GCAR) in 2012 and the other is that Visa's rules contain a general fines and penalties section. Defendants did not and cannot, however, show that either statement supports their attempt to rewrite the contract after the fact to make Third Party Fees or fees, fines, and penalties mean the same thing as liability for issuing bank losses. Rather, to get from the two statements to their result-driven, non-textual interpretation, Defendants push the boundaries of "advocacy" through the following five mischaracterizations, omissions, and conclusory assertions:

(1) After explaining why the limitation of liability exception does not apply to liability for issuer losses, Schnucks' prior briefs listed three examples of how Defendants could have written the contract differently if they wanted the exception to mean what they now claim it means. Defendants mischaracterize one-half of one of those examples (they ignore the other half of the example because MasterCard's ADCR program did not have a name change) as the primary premise of Schnucks' argument so they can incorrectly criticize Schnucks' argument for being based on a program they contend did not exist at the time the contract was signed.

(2) Defendants fail to acknowledge that the change from ADCR to GCAR was just a name change—when Visa's program was named ADCR in 2011 it still defined how Visa would determine the amount of issuing bank losses for which acquirers could be liable.[1] Schnucks should have used the former Visa program name in its example, but the example is still valid. There are no material differences between the Visa ADCR program and GCAR program. Beyond the failed attempt to create a "gotcha" moment, Defendants' Sur-Reply does not offer a rebuttal on the merits to this example or the other two.

(3) Defendants mischaracterize a general fines and penalties section in Visa's rules as a "preamble" to the 2011 ADCR program even though it stands as its own section, is not called a preamble, is separated from the ADCR rules by over 700 pages, states that it functions in addition to other enforcement provisions, and language in the ADCR rule shows that it is not subject to the general fines and penalties section.

[1] Visa changed the name of its program in 2012 to consolidate ADCR (which it used for cards issued by US issuing banks), Canadian Data Compromise Recovery Solution (DCRS) and the DCRS International Programs (which it used for cards issued by foreign issuing banks) into GCAR. *See Visa Global Compromised Account Recovery Program What Every Merchant Should Know About GCAR*, available at: http://usa.visa.com/download/merchants/what-every-merchant-should-know-GCAR-VOL-091213-final.pdf (last accessed July 23, 2014).

(4) Defendants' mislabeled the Visa general fines and penalties section "as a preamble to the ADCR program" so they could make a disjointed, incomplete, and flawed argument that the exception applies by deceptively implying a relationship (that does not actually exist in the rules) between Visa recovering actual issuer losses under the ADCR program and Visa's general ability to assess a fine or penalty for not complying with a Visa rule.

(5) Defendants summarily contend that reading the GCAR and ADCR rules "in context" shows that they are only process and procedure rules and, thus, "simply cannot" define the nature of the liability imposed. Defendants are wrong—the GCAR and ADCR rules create and define the liability of acquirers for issuer losses, in addition to identifying how the liability is calculated. Without the GCAR and ADCR rules, there would be no basis in the Visa or MasterCard rules for acquirer liability for issuer losses. Moreover, Visa and MasterCard distribute the amount they collect under those programs to affected issuers, which is in contrast to the fines and penalties that Visa and MasterCard retain for themselves.

Based on the foregoing, Defendants' Sur-Reply should be disregarded. The remainder of this response addresses in greater detail the areas Defendants' attempt to confuse.

I. ADCR TO GCAR WAS A CHANGE IN NAME ONLY

When Visa changed the name of its ADCR program to GCAR in 2012, the underlying substance and purpose of the rule remained the same. ADCR and GCAR both established Visa's right to collect money from an acquirer and distribute that money to reimburse issuers for the losses they incurred as a result of an account data compromise event. A comparison of the language of the rules before and after makes this obvious, including the opening sentences:

> **Account Data Compromise Recovery [ADCR] Process - U.S. Region**
>
> In the U.S. Region, the Account Data Compromise Recovery (ADCR) process allows Visa to determine the monetary scope of an account compromise event,

> collect from the responsible Member, and reimburse Members that have incurred *losses* as a result of the event.

(Ex. 1 to Defs' Sur-Reply, Doc. # 53-2, p. 759 (emphasis added).)

> **Global Compromised Account Recovery [GCAR] Program Overview (Updated) Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012,** an Issuer in Visa International or Visa Europe may recover a portion of its Incremental Counterfeit Fraud *losses* and operating expenses resulting from an Account Data Compromise Event involving a compromise of Magnetic-Stripe Data, and PIN data for events that also involve PIN compromise, under the Global Compromised Account Recovery (GCAR) program from an Acquirer(s) to whom liability for such *loss* has been assigned under the GCAR program.
>
> GCAR allows Visa to determine the monetary scope of an Account Data Compromise Event, collect from the responsible Acquirer(s), and reimburse Issuers that have incurred *losses* as a result of the event.

(Ex. 2 to Pl's Opp. and Partial Cross-Motion, Doc. # 44-2, p. 802 (emphasis added).)

II. SCHNUCKS PROPERLY RELIED ON THE 2012 VISA RULES

Defendants assert that Schnucks improperly relied on the current version of the Visa International Operating Regulations ("VIOR") because the current VIOR and Visa's current GCAR program did not exist when the parties negotiated and executed the Master Services Agreement.[2] Contrary to Defendants' argument, Schnucks is not relying on the "current version" of the VIOR.[3] Rather, Schnucks relied on and attached to its motion the relevant provisions of the October 2012 VIOR and the February 2013 MasterCard Security Rules and Procedures ("MasterCard Rules") because those are the rules MasterCard assessed Citicorp under and the rules that First Data relied on in setting a reserve for Visa liability.

[2] As explained above, Schnucks should have used "ADCR" instead of "GCAR" in the example of how Defendants could have drafted the exception in 2011. Notwithstanding this oversight, it is, appropriate to rely on the 2012 VIOR and the GCAR rules contained therein to demonstrate why the liability for issuer losses under GCAR does not fall under the exception to the limitation of liability.

[3] The "current version" of the VIOR is dated April 15, 2014, *available at*: http://usa.visa.com/download/merchants/Public-VIOR-15-April-2014.pdf (last accessed July 23, 2014). And there was a prior version to that dated October 15, 2013, *available at*: https://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf (last accessed July 23, 2014).

Schnucks used these versions of the rules to show that assessments under Visa's GCAR and MasterCard's ADCR program are not Third Party Fees or fees, fines or penalties—they are assessments of liability to reimburse issuers for their *losses*. This is true under Visa's 2011 ADCR program and after it was renamed as GCAR. (*See* Section I, *supra.*) ADCR states that the "process allows Visa to determine the monetary scope of an account compromise event, collect from the responsible Member, and reimburse Members that have incurred *losses* as a result of the event." (Ex. 1 to Defs' Sur-Reply, Doc. # 53-2, p. 759 (emphasis added).) And the ADCR process includes "Counterfeit Fraud Recovery" and "Operating Expense Recovery." (*Id.* at p. 760.) The bottom line is that there is no reference or support from the language of Visa's ADCR and GCAR programs that they are in any way a Third Party Fee or a fee, fine or penalty.

III. THERE ARE NO MEANINGFUL DIFFERENCES BETWEEN THE 2011 AND 2012 VISA RULES

Defendants claim to identify two differences between the 2011 and 2012 VIOR. Neither argument is factually accurate. First, they claim that the 2011 VIOR contains a "preamble reference to the terms 'fines' and 'penalties' that Visa used to characterize Visa's authority to impose all assessments (such as financial responsibility for a data breach) on an acquiring bank based on its merchant's conduct." (Defs' Sur-Reply at p. 3-4 (emphasis removed).) The second claimed difference is that in the 2011 VIOR, the ADCR program fell under the general "Counterfeit Losses" provisions, whereas in the 2012 VIOR, the GCAR program fell under its own data breach heading. (*Id.* at p. 4 n.3.) The same so-called "preamble"—a separate section known as the "Visa Right to Fine" section—is found in both the 2011 and 2012 VIOR. (*Compare* Ex. 1 to Defs.' Sur-Reply, Doc. # 53-2, p. 59, with Pl's Ex. 1 attached hereto, October 15, 2012 VIOR, p. 70.) And both the ADCR program and GCAR program fall under the same "Counterfeit Losses" provisions. (*Compare* Ex. 1 to Defs.' Sur-Reply, Doc. # 53-2, pgs. xvi & 758-765, with Pl's Ex. 1 attached hereto, October 15, 2012 VIOR, pgs. xxix & 800-806.)

Defendants use the purported "preamble" to argue that "the parties intended that any and all assessments by the Associations in enforcing their rules and regulations, as the Associations themselves described them as 'fines and penalties', are Schnucks' responsibility without limitation." (Defs' Sur-Reply at p. 4.) This is simply not true and Defendants are mistaken on several fronts. The "Visa Right to Fine" section, contrary to Defendants' argument, does not show the parties' intent that any and all assessments by the Associations are Schnucks' responsibility without limitation. In fact, the "Visa Right to Fine" provision further amplifies the distinction between losses under the GCAR/ADCR programs, and the separate fines and penalties Visa can impose for violating other provisions of the VIOR. The purported "preamble" to the ADCR program is not a preamble at all and appears 700 pages before the ADCR program. The purported "preamble" relates to a general right to assess fines and penalties for violating the VIOR, not ADCR. The absurdity of Defendants' argument can be shown by looking at the following language from the ADCR program: "Violations not involving a Transaction are resolved as specified in 'Visa Right to Fine' and as deemed appropriate by Visa." (Defs' Sur-Reply Ex. 2, p. 760.) This shows that the ADCR program is not governed by the "Visa Right to Fine" section—the very section that Defendants claim is a preamble and applies to the ADCR program. Defendants' argument is further undercut because the "Visa Right to Fine" section states: "These procedures and fines are in addition to enforcement rights under other provisions" of the VIOR. The ADCR provisions are an additional enforcement right—the right to collect amounts to reimburse affected issuing banks for their *losses*—losses which are not included in the limitation of liability exception in the MSA.

IV. ISSUER LOSS LIABILITY IS NOT A FEE, FINE, OR PENALTY

To manufacture a reason to point out the name change from ADCR to GCAR, Defendants claim that "Plaintiff's arguments are largely premised on Defendants' supposed failure to consider the language of the GCAR program when the parties drafted the exception to the limitation of liability contained in Section 5.4 of the MSA." (Defs' Sur-Reply at p. 3 (citing Plaintiff's Brief, Doc. # 44, at p. 18).) This is merely a distraction from the single question in this matter—whether liability for issuer losses falls under the limitation of liability exception. In its brief, after Schnucks explained why the plain language of the limitation of liability exception does not apply to liability for issuer losses, Schnucks provided three examples of how Defendants could have written the exception if they intended it to exclude from the limitation of liability all forms of monetary amounts they would become liable for after an account data compromise event. (Pl's Brief, Doc. # 44, at p. 18.)[4] One of the three examples was that Defendants could have inserted assessments according to the GCAR and ADCR regulations. (*Id.*) But they did not. (*Id.*)

In their opposition to Schnucks' Partial Cross-Motion, Defendants argued that they did not have to list GCAR and ADCR to make the exception apply to that liability. (Defs' Brief, Doc. #49, at p. 11.) Defendants' Sur-Reply did not reiterate that position. Rather, Defendants challenged one-half of one example in a list of three examples of how they could have written the exception. The basis of their argument is that they could not have referenced "GCAR" in the exception because "GCAR" did not exist in 2011, only the ADCR program did. MasterCard's

[4] These are the three examples from Schnucks reply that Defendants have yet to rebut:

> If Defendants, who are sophisticated entities, intended the second exception to exclude from the limitation of liability all forms of monetary amounts they might become liable for in the event of an account data compromise event at Schnucks, as they now claim, they could simply have said so. They could have added in the word 'losses' and written 'fines, fees, penalties or **losses** . . .' Or, they could have inserted the defined term 'Data Compromise Losses,' the definition of which encompasses all forms of financial liability arising from an account data compromise event (including losses and issuer reimbursements imposed by Visa and MasterCard). Or, they could have inserted 'assessments according to the GCAR and ADCR regulations.' But, they did not. Defendants used no words or defined terms in the exception evidencing intent to exclude from the $500,000 limitation of liability all forms of financial liability arising from an account data compromise event.

(Pl's Reply Brief, Doc. # 52, at p. 4.)

program was called ADCR in 2011 and now, but the Sur-Reply says nothing about their failure to list ADCR in the exception. Defendants also fail to explain to the court that the ADCR program in 2011 was essentially the same as the 2012 GCAR program.

While Defendants claim that this Court should disregard Schnucks' reliance on the language of GCAR and ADCR because Schnucks' "cherry-picked provisions for a self-serving purpose," they do not to explain what relevant provisions Schnucks failed to provide the Court. (Def's Sur-Reply at p. 5.) Schnucks provided the Court with only relevant provisions, including the entirety of the regulations relating to Visa's GCAR and MasterCard's ADCR programs. One would think that, if Defendants are going to make such an accusatory assertion, they would have at least provided some support.

Defendants further claim that "[w]hen read in proper context, the Visa ACDR (or current GCAR) and/or MasterCard's ADCR are only operating programs and procedures that the Associations use to calculate the fines and penalties levied against an acquiring bank as a result of its' merchant's violation of the various security rules." (*Id.* at p. 5.) How they come to come to this conclusion is a mystery. By "context" they appear to mean how Defendants' wish it to be read. As explained above, fines and penalties are not mentioned in the Visa ACDR (or current GCAR) or MasterCard ADCR. These programs assess liability to reimburse issuers for their losses.

V. GCAR AND ADCR CREATE THE LIABILITY FOR ISSUER LOSSES

Finally, without any support, Defendants argue that the Visa's ADCR (and GCAR) and MasterCard's ADCR "are not characterizations of the *nature* of the financial responsibility itself," but, rather, "merely detail the processes and procedures that the Associations use to assess financial responsibility [ ] for a data breach." (*Id.* at p. 5-6 (emphasis in original).)

Defendants then, again without any support, assert that "[a] process and procedure simply cannot define the *nature* of the financial responsibility that the Associations impose as a result of a data compromise event." (*Id.* at p. 6 (emphasis in original.) Defendants fail to explain why this is the case or cite any authority. Again, Defendants are merely stating what the wish the case to be. Without the GCAR and ADCR programs, there would be no obligation owed by acquirers to reimburse issuers for their losses from an account data compromise event. By reading the actual language of the GCAR and ADCR programs, it is evident that they establish both the nature of the liability as well as the process by which the amount is collected from an acquirer and distributed to issuers.

VI. CONCLUSION

Based upon the foregoing and the arguments made in its prior briefs, Schnucks respectfully request that this Court grant its Partial Cross-Motion for Judgment on the Pleadings; deny Defendants' Motion for Judgment on the Pleadings; dismiss Defendants' Counterclaim; and grant judgment to Schnucks on its declaratory judgment claim.

Dated: July 25, 2014

Respectfully submitted,

By: /s/ *Kevin F. Hormuth*
Kevin F. Hormuth, No. 48165 MO
David P. Niemeier, No. 50969 MO
GREENSFELDER, HEMKER & GALE, PC
10 South Broadway, Suite 2000
St. Louis, MO 63102
kfh@greensfelder.com
dpn@greensfelder.com
Telephone: 314.241.9090
Facsimile: 314.345.5466

Craig A. Hoffman (*pro hac vice*)
cahoffman@bakerlaw.com
Telephone: 513.929.3491
Facsimile: 513.929.0303

Attorneys for Plaintiff Schnuck Markets, Inc.

CERTIFICATE OF SERVICE

I certify that on the 25th of July, 2014, the foregoing *Plaintiff's Response to Defendants' Sur-Reply Memorandum* was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

By: /s/ *Kevin F. Hormuth*
Kevin F. Hormuth

EXHIBIT 1

VISA

Visa International Operating Regulations

15 October 2012

Member Response Standards - CEMEA Region

A CEMEA Member must respond to a request from another CEMEA Member, Visa, or a law enforcement agency

ID#: 111011-010410-0002249

Merchant Investigation Responsibilities

Investigation of Merchant Outlet

Visa may contact a Merchant Outlet directly and conduct an onsite investigation of the Merchant Outlet at any time.

If the Merchant fails to correct a violation identified by Visa, Visa may, for reasons such as those listed in "Visa Right to Terminate Merchant, Payment Service Provider, or Sponsored Merchant," impose conditions upon the Merchant or permanently prohibit the Merchant, or its principals, from participating in the Visa or Visa Electron Program.

ID#: 111011-010410-0007429

Operating Regulations Compliance and Enforcement

Fines and Penalties - General

Visa Right to Fine

The *Visa International Operating Regulations* contain enforcement mechanisms that Visa may use for violations of the *Visa International Operating Regulations*. The Operating Regulations also specify the procedure for the allegation and investigation of violations and the rules and schedules for fines and penalties.

Visa may levy fines and penalties as specified in the *Visa International Operating Regulations.* Visa officers will enforce these fines and penalties.

These procedures and fines are in addition to enforcement rights available to Visa under other provisions of the *Visa International Operating Regulations*, the applicable Certificate of Incorporation and Bylaws, or through other legal or administrative procedures.

ID#: 010410-010410-0007280

General Fines Schedule (Updated)

The fines listed in the table below are in addition to any other fines or penalties specified in the *Visa International Operating Regulations*.

General Schedule of Fines

Violation	Fine
First violation of regulation	Warning letter with specific date for correction and US $1,000 fine
Second violation of same regulation in a 12-month period after Notification of first violation	US $5,000 fine
Third violation of same regulation in a 12-month period after Notification of first violation	US $10,000 fine
Fourth violation of same regulation in a 12-month period after Notification of first violation	US $25,000 fine
5 or more violations of same regulation in a 12-month period after Notification of first violation	Visa discretion
If the 12-month period is **not** violation-free and the fines total US $25,000 or more	Additional fine equal to all fines levied during that 12-month period

ID#: 151012-010410-0000482

Fines and Penalties Process

Determination of Violation

Determination of a violation of the *Visa International Operating Regulations* may be made as follows:

- Based on the response from a Member to a Notification of investigation and other available information, Visa will determine whether a violation of the *Visa International Operating Regulations* has occurred.
- The Member's failure to respond to a Notification of investigation and to provide all information requested may result in a determination that a violation has occurred.

ID#: 010410-010410-0001052

Notification of Determination

Visa will notify a Member if it determines that a violation has occurred, or if it determines that a violation is continuing to occur, and will specify a date by which the Member must correct the violation. The Notification will advise the Member of the:

- Reasons for such determination
- Fines assessed
- Right to appeal the determination and/or the fines assessed for such violation

Visa may require a Member to submit a compliance plan to resolve the violation.

ID#: 160312-010410-0001053

Fine Assessment

All fines imposed by Visa are fines imposed on Members. A Member is responsible for paying all fines, regardless of whether it absorbs the fines, passes them on, or increases them in billing its customer (e.g., Cardholder, Merchant). A Member must **not** represent to its customer that Visa imposes any fine on its customer.

ID#: 010410-010410-0001054

Collection of Fines

Visa will electronically collect all fines through Visa billing statements after notifying the Member.

ID#: 160312-010410-0002449

Allegations and Investigations

Allegations of violations of the *Visa International Operating Regulations* may be brought to Visa's attention by:

- A Member
- An Agent or a VisaNet Processor, through its registering Member
- A Visa Officer

Visa may investigate allegations of violations of the *Visa International Operating Regulations*.

ID#: 160312-010410-0007366

Notification Response

A Member must respond to and provide information requested by Visa for a *Visa International Operating Regulations* violation that is under investigation.

The Member must submit its response and information, within the time period specified, by mail, courier, facsimile, hand, e-mail, or other electronic delivery method. The Notification response is effective when posted, sent, or transmitted by the Member or its Agent to Visa.

ID#: 160312-150211-0025974

Fines and Penalties for Repetitive and Willful Violation

Repetitive Violations

Repetitive violations of the *Visa International Operating Regulations* incur heavier fines or other actions. A violation of any section qualifies as a repetitive violation only if the violating Member does not correct it by the date specified in the Notification.

ID#: 010410-010410-0003645

Time Period

Penalties increase for repetitive violations within any 12-month period. The 12-month period begins on the date of the most recent Notification of the violation and ends following a 12-month period free of violations of that regulation.

ID#: 010410-010410-0000478

Willful Violations

In addition to the fines and penalties specified in "Fines and Penalties - General," a Member found to have willfully violated the *Visa International Operating Regulations*, adversely affecting the goodwill associated with the Visa system, brand, products and services, the operation of the Visa Systems, or the operations of other Members, will be subject to a further fine. A violation is considered "willful" if the Member knew, or should have known, or its knowledge can be fairly implied, that its conduct constituted a violation of the *Visa International Operating Regulations*.

When determining the amount of a fine, in addition to the criteria above, the following will be considered:

- Type of violation
- Nature of the damage, including the amount incurred by Visa and its Members
- Repetitive nature of the violation
- Member history or prior conduct

- Effect of the assessment upon the safety and soundness of the Visa system and the Member, including the Member committing the violation
- Any other criteria Visa deems appropriate

ID#: 160312-010410-0007288

Compliance - General

Compliance Programs - General

Visa rights and Member obligations for specific compliance programs, specified in "Compliance Monitoring," follow the basic structure of fines described in "Operating Regulations Compliance and Enforcement."

ID#: 010410-010410-0007040

Compliance Enforcement Appeals

Enforcement Appeals

A Member may appeal[4] a determination of a violation or fine to Visa as follows:

- The Member's appeal letter must be received by Visa within 30 days of the Member's receipt of the Notification of the violation or fine.
- The appealing Member must submit with the appeal any new or additional information necessary to substantiate its request for an appeal.
- A fee of US $5,000 will be assessed to the Member upon receipt of the appeal. This fee is refundable if the appeal is upheld.

Visa bases its decision on the new information provided by the requesting Member. Each Member may submit arguments supporting its position. All decisions are final and not subject to any challenge.

ID#: 160312-150211-0025975

[4] Appeal procedures are available from Visa upon request.

- Inadvertently left at a Merchant Outlet
- A Non-Reloadable Visa Prepaid Card recovered without an Issuer's request or in the absence of a Pickup Response

ID#: 151012-010410-0002192

Recovered Card Rewards - Suspicious Circumstances - U.S. Region

A U.S. Acquirer must pay the Merchant a reward of at least US $100 if a recovered Visa Card or Visa Electron Card was **not** listed in the Exception File with a Pickup Response and the Merchant's request for Authorization was due to either:

- Suspicious circumstances (Code 10 Authorization)
- Presentation of a Visa Card or Visa Electron Card on which the first 4 digits of the embossed or printed Account Number (if applicable) do not match the 4 digits printed above or below the Account Number

ID#: 010410-010410-0001773

Reimbursement of Recovered Card Rewards - U.S. Region

A U.S. Issuer must reimburse the Acquirer for the amount of a reward paid for Card recovery, up to US $100.

Reimbursement of a reward payment must not exceed US $250 per instance of multiple Visa Card or Visa Electron Card recovery.

ID#: 010410-010410-0008056

Counterfeit Losses

Counterfeit Transaction Liability

Assignment of Liability for Counterfeit Transactions

Visa assigns liability to the Issuer or Acquirer for counterfeit Transactions, based on the following priorities in the order shown:

- The Acquirer, if the Merchant identified on a Risk Identification Service Chargeback Exception Report contributed to the origination of the Counterfeit Transaction Receipt [122]
- The Acquirer first receiving the Counterfeit Transaction Receipt, if the BIN is **not** assigned to a Member

- The Acquirer that submitted the Transaction into Interchange, if an Authorization was required and **not** obtained **or** the Account Number encoded on the Magnetic Stripe of a Visa Card or Visa Electron Card was authorized but was different than the embossed or printed Account Number submitted into Interchange [123]
- The Issuer identified by the manufacturer product information printed on the reverse side of the Visa Card or Visa Electron Card, if the counterfeit Visa Card or Visa Electron Card was recovered and resulted from either the loss or theft of an unembossed and unencoded Visa Card or unencoded Visa Electron Card bearing the Visa Program Marks [124]
- The Issuer, if its BIN appears on the Counterfeit Transaction Receipt or the BASE II Clearing Record for the counterfeit Transaction [125]

ID#: 050411-010410-0001812

Issuer Identification on Card

Visa identifies the Issuer that ordered the manufacture of a Visa Card or Visa Electron Card by either the name printed on the Visa Card or Visa Electron Card or the manufacturer product information printed on the back of the Visa Card or Visa Electron Card.

There is no time limit on a Member's right to reassign liability to the Issuer under this section.

ID#: 010410-010410-0008158

Counterfeit Card Transaction Reporting

If a Member discovers Counterfeit Card activity, the Member must immediately report the Account Number to Visa.

ID#: 010410-010410-0001816

[122] For qualifying Transactions, the EMV Liability Shift, as specified in "EMV Liability Shift Participation," takes precedence over this section to assess liability in the event of a conflict.

[123] For qualifying Transactions, the EMV Liability Shift, as specified in "EMV Liability Shift Participation," takes precedence over this section to assess liability in the event of a conflict.

[124] For qualifying Transactions, the EMV Liability Shift, as specified in "EMV Liability Shift Participation," takes precedence over this section to assess liability in the event of a conflict.

[125] For qualifying Transactions, the EMV Liability Shift, as specified in "EMV Liability Shift Participation," takes precedence over this section to assess liability in the event of a conflict.

Global Compromised Account Recovery (GCAR)

Global Compromised Account Recovery Program Overview (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, an Issuer in Visa International or Visa Europe may recover a portion of its Incremental Counterfeit Fraud losses and operating expenses resulting from an Account Data Compromise Event involving a compromise of Magnetic-Stripe Data, and PIN data for events that also involve PIN compromise, under the Global Compromised Account Recovery (GCAR) program from an Acquirer(s) to whom liability for such loss has been assigned under the GCAR program.

GCAR allows Visa to determine the monetary scope of an Account Data Compromise Event, collect from the responsible Acquirer(s), and reimburse Issuers that have incurred losses as a result of the event.

GCAR allows recovery of counterfeit transaction losses across all Visa-owned brands (i.e., Visa, Interlink, Plus, and Visa Electron) when a violation, attributed to another Visa Member, could have allowed Magnetic-Stripe Data (and PIN data, if applicable) to be compromised and the subsequent financial loss was associated with **any** of the following:

- A Visa Transaction
- An Interlink transaction
- A Plus Transaction
- A Visa Electron Transaction

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, the GCAR program is only available when:

- There has been a violation involving non-compliance with one or more of the following:
  - Payment Card Industry Data Security Standard (PCI DSS)
  - PIN Management Requirements Document
  - *Visa PIN Security Program Guide*
- The violation could allow a compromise of contents of any track on the Magnetic Stripe (and PIN data, if applicable) for a Visa Transaction, a Plus Transaction, an Interlink transaction, or a Visa Electron Transaction

ID#: 151012-150512-0026564

GCAR Qualification (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will determine Account Data Compromise Event qualification, Counterfeit Fraud Recovery and Operating Expense Recovery amounts, Issuer eligibility, and Acquirer liability under the Global Compromised Account Recovery (GCAR) program, in accordance with the *Visa Global Compromised Account Recovery (GCAR) Guide*.

To qualify an Account Data Compromise Event under GCAR, Visa must determine that all of the following criteria have been met:

- A Payment Card Industry Data Security Standard (PCI DSS), PIN Management Requirements Documents, or *Visa PIN Security Program Guide* violation has occurred that could have allowed a compromise of Account Number and Card Verification Value (CVV) Magnetic-Stripe Data, and PIN data for events also involving PIN compromise
- Account Number and CVV Magnetic-Stripe Data has been exposed to a compromise
- 15,000 or more eligible accounts were sent in CAMS Internet Compromise (IC) and/or Research and Analysis (RA) alerts indicating Account Number and CVV Magnetic-Stripe Data is potentially at risk
- A combined total of US $150,000 or more Counterfeit Fraud Recovery and Operating Expense Recovery for all Issuers involved in the event
- Elevated Magnetic-Stripe counterfeit fraud was observed in the population of eligible accounts sent in the CAMS Alert(s) associated with the Account Data Compromise Event

ID#: 151012-150512-0026565

GCAR - Preliminary Determination of Event Qualification

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, following preliminary fraud analysis and investigation of an Account Data Compromise Event, Visa will provide the Acquirer(s) with:

- Findings in support of the preliminary determination that the event is qualified for the Global Compromised Account Recovery (GCAR) program
- A preliminary estimate of counterfeit fraud and operating expense liability amounts

ID#: 160312-150512-0026566

GCAR - Appeal Rights

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, an Acquirer may appeal a Global Compromised Account Recovery (GCAR) preliminary determination of Account Data Compromise Event qualification to Visa by submitting an appeal letter. The appeal letter must:

- Be received by Visa within 30 calendar days of the Acquirer's receipt of the preliminary Notification of qualification and estimated liability
- Include written arguments and supporting information for the appeal

Visa will notify the Acquirer of the final disposition of the appeal. The decision on the appeal is final and not subject to any challenge or any other appeal rights.

The appeal rights as specified in "Enforcement Appeals" are not applicable to GCAR.

ID#: 160312-150512-0026567

GCAR - Appeal Fee (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will collect from the Acquirer through the Global Member Billing System a Global Compromised Account Recovery (GCAR) appeal fee, as specified in the applicable Fee Guide.

ID#: 151012-150512-0026568

GCAR - Notification of Final Liability and Recovery Amounts

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will notify the Acquirer(s) deemed responsible for an Account Data Compromise Event of its final counterfeit fraud and operating expense liability amounts under Global Compromised Account Recovery (GCAR).

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will notify the affected Issuers that an Account Data Compromise Event qualifies for Operating Expense Recovery and Counterfeit Fraud Recovery under GCAR, and advise them of their recovery amounts.

ID#: 160312-150512-0026569

GCAR - Debits, Credits, and Fees (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa will submit debits to the Acquirer(s) responsible for an Account Data Compromise Event and credits, less administrative fees, to eligible Issuers through the Global Member Billing System. Visa retains a Global Compromised Account Recovery (GCAR) program administration fee, as specified in the applicable Fee Guide. The debit and credit amounts as determined by Visa are final and not subject to any appeal or other challenge.

ID#: 151012-150512-0026570

GCAR - Non-Cooperation Analysis Fee (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Visa assesses to the Acquirer through the Global Member Billing Systems, a Global Compromised Account Recovery (GCAR) program non-cooperation analysis fee, as specified in the applicable Fee Guide, if the Acquirer, its Merchant, or other Compromised Entity refuses to allow a forensics investigation.

ID#: 151012-150512-0026571

GCAR - Conditions for Reimbursement

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, reimbursements under the Global Compromised Account Recovery (GCAR) program to affected Issuers are based solely upon the ability of Visa to collect the counterfeit fraud and operating expense liability amounts from the responsible Acquirer(s).

ID#: 160312-150512-0026572

GCAR - Catastrophic Loss

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, if an Account Data Compromise Event is deemed catastrophic, Visa reserves the right to implement an alternative process to the Global Compromised Account Recovery (GCAR) program.

ID#: 160312-150512-0026573

GCAR Program Compliance (Updated)

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, a Member must comply with the *Visa Global Compromised Account Recovery (GCAR) Guide.*

ID#: 151012-150512-0026749

GCAR Incremental Fraud Recovery

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, to determine Incremental Fraud Recovery, the Global Compromised Account Recovery (GCAR) program:

- Uses an Incremental Counterfeit Fraud calculation that is based on actual counterfeit fraud reported in excess of the Issuer's baseline counterfeit fraud during an alert's Fraud Window. The Issuer baseline is determined at the BIN level and calculated for each alert based on a set methodology.

- Uses an Issuer Counterfeit Fraud Recovery limit to incent effective management of fraud. Issuer counterfeit fraud reported in excess of US $3,000 per account will be excluded from Incremental Counterfeit Fraud recovery calculations.
- Excludes from the Issuer recovery calculation Transactions that have been successfully charged back by the Issuer and for which the Acquirer has not submitted a successful Representment at the time of the calculation
- Includes in the Issuer recovery calculation fraud Transactions that occurred up to 12 months prior to and one month following the CAMS date

Counterfeit fraud Transactions must have been authorized through VisaNet to be eligible for GCAR recovery. The only exception to this rule is that on-us[126] ATM counterfeit fraud Transactions on Plus accounts will be eligible for GCAR recovery if the Issuer is in a country where at least 95% of domestic volume of Visa-owned brands (excluding on-us ATM) is authorized through VisaNet.

ID#: 160312-150512-0026751

GCAR Operating Expense Recovery

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, Operating Expense Recovery under the Global Compromised Account Recovery (GCAR) program is US $2.50 per eligible account on Internet Compromise (IC) and/or Research and Analysis (RA) CAMS-alerted accounts that were not identified as expired at the time of the CAMS Alert.

ID#: 160312-150512-0026752

GCAR General Calculation Rules

Effective for Qualifying CAMS Events or VAB Events in which the first or only alert is sent on or after 15 May 2012, the following general rules are applicable for Global Compromised Account Recovery (GCAR) calculations:

- Issuers must use CAMS to be eligible for recovery
- Accounts must have been authorized through VisaNet in a Transaction processed through the Compromised Entity during the Account Data Compromise Event timeframe to be included in Acquirer liability and Issuer recovery calculations
- Accounts included in a different CAMS Alert in the prior 12 months are excluded from the Acquirer liability and Issuer recovery calculations
- Visa reserves the right to adjust an Acquirer's total liability for an Account Data Compromise Event

ID#: 160312-150512-0026753

[126] An On-Us Transaction is a Transaction where the Issuer and the Acquirer are the same Member.

Account Data Compromise Recovery (ADCR) - U.S. Region

Account Data Compromise Recovery Process Description - U.S. Region (Updated)

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, the Account Data Compromise Recovery (ADCR) process allows Visa to determine the monetary scope of an account compromise event, collect from the responsible Member, and reimburse Members that have incurred losses as a result of the event.

ADCR allows the recovery of counterfeit transaction losses across all Visa-owned brands (i.e., Visa, Interlink, and Plus) when a violation attributed to another Visa Member could have allowed data to be compromised and the subsequent financial loss was associated with any of the following:

- A Visa Transaction
- An Interlink transaction
- A Plus transaction

This process is only available when there has been a violation of at least one of the following:

- Operating Regulations involving electronic storage of the full contents of any track on the Magnetic Stripe subsequent to Authorization of a Transaction
- Operating Regulations involving non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) that could allow a compromise of the full contents of any track on the Magnetic Stripe
- Operating Regulations involving the PIN Management Requirements Documents that could allow a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to Authorization

The Account Data Compromise Recovery process includes:

- Counterfeit Fraud Recovery
- Operating Expense Recovery

ID#: 151012-010410-0000877

Transactions Excluded from ADCR Process - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, violations of the *Visa International Operating Regulations* not involving storage of Magnetic-Stripe Data are excluded from this process.

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, violations not involving non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) that could allow a compromise of the full contents of any track on the Magnetic Stripe are excluded from this process.

Effective for Qualifying CAMS Events sent on or before 14 May 2012, violations not involving a Transaction are resolved as specified in "Visa Right to Fine" and as deemed appropriate by Visa.

ID#: 160312-010410-0000878

Determination of ADCR Eligibility - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, following the fraud analysis and investigation of the compromise event, the U.S. Member is provided with:

- Findings in support of the preliminary determination that the event is eligible for the ADCR process
- Any estimated counterfeit fraud and operating expense liability amounts

ID#: 160312-010410-0009035

Counterfeit Fraud Recovery Process - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, a U.S. Member is compensated for a portion of its counterfeit fraud losses incurred as the result of a Magnetic-Stripe Data account compromise event. The Counterfeit Fraud Recovery process is initiated by Visa when:

- An account compromise event occurs
- A Compromised Account Management System (CAMS) Alert, or multiple CAMS Alerts for the same account compromise event, is sent to affected Members
- The account compromise event involves at least 10,000 Account Numbers **and** a combined total of US $100,000 or more recovery for all Issuers involved in the event
- At least one of the following:
  - The full contents of any track on the Magnetic Stripe was stored subsequent to Authorization of a Transaction
  - A violation of the Payment Card Industry Data Security Standard (PCI DSS) could have allowed a compromise of the full contents of any track on the Magnetic Stripe
  - A violation of the PIN Management Requirements Documents could have allowed a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to Authorization
- Incremental fraud is attributed to the particular account compromise event

ID#: 160312-010410-0000880

Counterfeit Fraud Reimbursement Conditions - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, only counterfeit fraud properly reported as specified in the *Visa International Operating Regulations* is considered when determining any reimbursement due.

ID#: 160312-010410-0000881

Baseline Counterfeit Fraud Level Determination - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, Visa determines a baseline counterfeit fraud level by analyzing reported Magnetic-Stripe-read counterfeit fraud losses that occurred up to 12 months before a Qualifying CAMS Event date and one month after the Qualifying CAMS Event date.

ID#: 160312-010410-0000882

Counterfeit Fraud Recovery Eligibility - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, U.S. Members are eligible for Counterfeit Fraud Recovery when there is incremental counterfeit fraud activity above the baseline counterfeit fraud level, as determined by Visa.

ID#: 160312-010410-0000883

Counterfeit Fraud Recovery Process - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, the U.S. Member deemed responsible for an account compromise event is notified of its estimated counterfeit fraud liability.

After the deadline for fraud reporting has passed, a Member communication broadcast is used to notify affected U.S. Members that an account compromise event qualifies for Counterfeit Fraud Recovery and advises them of their recovery amount.

The U.S. Member deemed responsible for the account compromise event is then notified of its actual counterfeit fraud liability.

ID#: 160312-010410-0008117

ADCR Reimbursement Guidelines - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, the following rules are related to the recovery process in the U.S. Region:

- Only recovery amounts of US $25 or more are collected and distributed to affected U.S. Members.
- Only U.S. Members that were registered to receive CAMS Alerts at the time of the first CAMS Alert for the event that is the subject of the ADCR proceeding are eligible to receive counterfeit fraud reimbursement.
- Counterfeit fraud losses on Account Numbers that were included in a different Qualifying CAMS Event within the 12 months before the Qualifying CAMS Event date are excluded.

- If 2 or more Qualifying CAMS Events occur within 30 days of each other, and the events each involve a minimum of 100,000 Account Numbers, the responsible U.S. Members share liability for the counterfeit fraud amount attributed to the accounts in common.

ID#: 160312-010410-0000887

Counterfeit Fraud Liability Collection and Distribution - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, counterfeit fraud liability is collected from the responsible U.S. Member(s) through the Global Member Billing Solution. Funds are distributed the following month, at the Business ID level, through the Global Member Billing Solution, to affected Members.

ID#: 160312-010410-0000888

ADCR Administrative Fees - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, an administrative fee is charged to the Issuer for each reimbursement issued, as specified in the *Visa U.S.A. Fee Guide*.

ID#: 160312-010410-0000889

Operating Expense Recovery Process - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, a U.S. Member enrolled in the Operating Expense Recovery process is compensated for a portion of its operating expenses incurred as a result of a Magnetic-Stripe Data account compromise event. The Operating Expense Recovery process is initiated by Visa when:

- An account compromise event occurs
- A CAMS Alert, or multiple CAMS Alerts for the same account compromise event, is sent to affected Members
- The account compromise event involves at least 10,000 Account Numbers **and** a combined total of US $100,000 or more recovery for all Issuers involved in the event
- At least one of the following:
  - The full contents of any track on the Magnetic Stripe were stored subsequent to Authorization of a Transaction
  - A violation of the Payment Card Industry Data Security Standard (PCI DSS) could have allowed a compromise of the full contents of any track on the Magnetic Stripe
  - A violation of the PIN Management Requirements Documents could have allowed a compromise of PIN data for a Visa Transaction, a Plus transaction, or an Interlink transaction subsequent to Authorization

ID#: 160312-010410-0000890

Operating Expense Recovery Enrollment - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, U.S. Members must complete the one-time Operating Expense Recovery enrollment process to be eligible to receive operating expense reimbursement. Members may enroll at any time but are only eligible for operating expense reimbursement for Qualifying CAMS Events that occur after enrollment is complete. Members not enrolled prior to a Qualifying CAMS Event date are **not** eligible to receive operating expense reimbursement.

ID#: 160312-010410-0000891

Operating Expense Liability Notification - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, the U.S. Member deemed responsible for an account compromise event is notified of its estimated operating expense liability.

A Member communication broadcast is used to notify affected U.S. Members enrolled in the Operating Expense Recovery process that an account compromise event qualifies for Operating Expense Recovery and advises them of their recovery amount.

The U.S. Member deemed responsible for the account compromise event is then notified of its actual operating expense liability.

ID#: 160312-010410-0008116

Operating Expense Recovery Conditions - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, the following rules are related to the recovery process in the U.S. Region:

- Only recovery amounts of US $25 or more are collected and distributed to affected U.S. Members enrolled in the Operating Expense Recovery process.
- Only U.S. Members that were registered to receive CAMS Alerts at the time of the first CAMS Alert for the event that is the subject of the ADCR proceeding are eligible to receive operating expense reimbursement.
- Operating expenses for Account Numbers that were included in a different Qualifying CAMS Event within the 12 months before the CAMS Event date are excluded.
- If 2 or more Qualifying CAMS Events occur within 30 days of each other, and the events each involve a minimum of 100,000 Account Numbers, the responsible U.S. Members share liability for the operating expense attributed to the accounts in common.

ID#: 160312-010410-0000895

Operating Expense Liability Collection and Distribution - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, operating expense liability is collected from the responsible U.S. Member(s) through the Global Member Billing Solution. Funds are distributed the following month, at the Business ID level, through the Global Member Billing Solution to affected Members enrolled in the Operating Expense Recovery process.

ID#: 160312-010410-0000896

Operating Expense Recovery Administration Fee - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, an administrative fee is charged to the Issuer for each reimbursement issued, as specified in the *Visa U.S.A. Fee Guide*.

ID#: 160312-010410-0000897

Operating Expense Reimbursement Conditions - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, reimbursements to affected U.S. Members are based solely upon the ability of Visa to collect the counterfeit fraud and operating expense liability amounts from the responsible Member.

ID#: 160312-010410-0000898

Catastrophic Account Compromise Event - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, if an account compromise event is deemed catastrophic, Visa reserves the right to implement an alternative process.

ID#: 160312-010410-0008929

ADCR Appeal - U.S. Region

Effective for Qualifying CAMS Events sent on or before 14 May 2012, a U.S. Member may appeal a determination of eligibility to Visa by submitting an appeal letter. The appeal letter must:

- Be received by Visa within 30 calendar days of the Member's receipt of the Notification of eligibility and estimated liability
- Include written arguments and supporting information for the appeal

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, the appeal rights, as specified in "Enforcement Appeals - U.S. Region," are not applicable to ADCR.

Effective for Qualifying CAMS Events sent on or before 14 May 2012, Visa will notify the U.S. Member of the final disposition of the appeal.

Effective for Qualifying CAMS Events sent on or before 14 May 2012, in the U.S. Region, the decision on any appeal is final and **not** subject to any challenge.

Effective for Qualifying CAMS Events sent on or before 14 May 2012, Visa will collect from the U.S. Member an appeal fee, as specified in the *Visa U.S.A. Fee Guide,* through the Global Member Billing Solution. For a data compromise event that qualifies under both the ADCR process and the international Data Compromise Recovery solution, Visa will collect only one appeal fee from the Member, as specified in the *Visa U.S.A. Fee Guide.*

ID#: 160312-010410-0009036

Data Compromise Recovery Solution (DCRS)

Data Compromise Recovery Solution Overview

Effective for Qualifying CAMS Events or VAB Events sent on or before 14 May 2012, an Issuer of Visa International or Visa Europe may recover incremental counterfeit fraud losses resulting from a Data Compromise event involving theft of full Magnetic-Stripe Data under the Data Compromise Recovery solution from Member(s) to whom liability for such loss has been assigned pursuant to the Data Compromise Recovery solution.

ID#: 160312-010410-0003334

Data Compromise Recovery Solution Eligibility

Effective for Qualifying CAMS Events or VAB Events sent on or before 14 May 2012, Visa will determine a data compromise event, fraud, and Issuer eligibility under the Data Compromise Recovery Solution.

ID#: 160312-010410-0003335

Data Compromise Event Eligibility (Updated)

Effective for Qualifying CAMS Events or VAB Events sent on or before 14 May 2012, Visa will determine data compromise event eligibility based on:

- Forensic confirmation or preponderance of evidence that a breach exists
- A violation of the Payment Card Industry Data Security Standard (PCI DSS) occurred that could allow a compromise of account data
- Full Magnetic Stripe counterfeit fraud occurred on a portion of exposed Account Numbers